



## Best Practices for Employers Offering Personal Health Records (PHRs)

### Health Privacy Project

December 2007

Personal health records (PHRs) have the potential to help individuals better manage their own health. But the ability to access personal health information raises concerns about privacy -- especially concerning employer access to employee health information.

While a number of companies already offer PHRs, consumer concerns about privacy safeguards and regulatory uncertainty persist. To address these issues directly, the Health Privacy Project, together with CHCF and IBM, convened an Employers' Working Group on PHRs. Through a collaborative process, they developed *Best Practices for Employers Offering Personal Health Records*.

These best practices are intended to serve as aspirational guidelines for employers, not a one-size-fits-all solution, as companies develop and implement their own PHR-related policies and practices.

Members of the Employers' Working Group on PHRs include representatives from the following companies and organizations: Center for Democracy and Technology; Dell; Google; Hewitt Associates; IBM; Markle Foundation; Omnimedix Institute; Pfizer; Pitney Bowes; Revolution Health; Wal-Mart; and WebMD.

### The Ten Best Practices

1. **Transparency and notice.** Employers should be transparent about their reasons for offering a PHR to employees and all policies that apply to the PHR. Employers should provide an Information Policy Statement or Notice that clearly lays out the ways in which information in the PHR will be used and safeguarded. Employers should incorporate the Notice into their health benefit programs, and should make it available in a layered format -- a short concise version to accompany a more detailed one. Employees should be informed of any updates to the policy.
2. **Education.** Employees should be educated about the benefits, functions, and content of the PHR. Information about the PHR should be communicated in numerous ways to build both knowledge and trust.
3. **Employees can choose which content is included in the PHR.** Employees should be able to determine the content of the PHR, including which providers and plans contribute to it. Employees should be able to annotate the records submitted by others, as well as to enter their own information, with employee-entered data marked as such. The identification of sources of all personal health information in the PHR should be readily apparent.
4. **Employees control access to and use of the PHR.** A. Employees should control who is allowed to access their PHRs. Employers should not access or use employees' individually-identifiable health information from the PHR. B. Employees should choose, without condition, whether to grant access to personal health information within their PHRs for any "secondary uses." An audit trail that shows who has accessed the PHR should be easily available to employees.
5. **Employees can designate proxies to act on their behalf.** Employees should determine who, including family members and caregivers, should have direct access to their PHRs on their behalf. Where possible, employees should be able to grant proxy access to full or partial information in their PHRs, including access in emergency circumstances. Employees should also have the ability to revoke access privileges.
6. **"Chain of trust": Information policies extend to business partners.** The information policies and practices of employer-sponsored PHRs should follow the data through chain of trust agreements that require business partners to adhere to the employer's applicable policies and practices.
7. **Data security.** Employers should provide a strong level of security to safeguard the information in the PHR systems. A robust authentication process for access to PHRs should be required, in addition to an audit trail that shows who has accessed information and when.
8. **Data management.** Employers should ensure that the PHR systems they provide have comprehensive data management strategies that protect the integrity of the data and include data retention policies.

9. **Enforcement and remedies.** Employers should establish oversight and accountability mechanisms for adhering to their PHR policies and practices. Employers should put into place a mechanism to promptly notify employees of any inappropriate access to or use of information contained in an employee's PHR, identify the steps which have been taken to address the inappropriate activity, and make resources available to employees to assist them in addressing the effects of the inappropriate activity.
10. **Portability.** Employers should offer PHRs that are portable, to the extent feasible, allowing employees to maintain or move the PHR and/or the data it contains even after employment or coverage ends or changes.

An overview of the best practices is available on the Health Privacy Project Web site through the link below.

## Related CHCF Pages

 [HTML Personal Health Records: Employers Proceed with Caution](#)

 [HTML National Consumer Health Privacy Survey 2005](#)

## External Links

[Health Privacy Project Web Site](#)

**California HealthCare Foundation**  
1438 Webster Street Suite 400, Oakland, CA 94612  
Tel: 510.238.1040 Fax: 510.238.1388

© 2007 California HealthCare Foundation. All Rights Reserved.